리눅스 서버 환경에서 네트워크 침해 대비를 위한 VPN 기술 분석

이재웅* · 정성재** · 배유미** · 이광용** · 장래영* · 소우영*

*한남대학교 컴퓨터공학과, **(주)엔버

VPN technology analysis: How to protect against network attacks in a Linux environment

Jae-Ung Lee* · Sung-Jae Jung** · Yu-Mi Bae** · Kwang-Yong Lee** · Rae-Young Jang* · Woo-Young Soh*

**Hannam University, **Enber Co., Ltd

E-mail : leejaeung1990@gmail.com, posein@naver.com, yumidw@hanmail.net, kylee@enber.net, jangraeyoung@hnu.kr, wsoh@hnu.kr

요 약

초기의 해커들은 시스템 장애, 파괴가 목적이었으나 최근에는 기업들이 가지고 있는 고객의 개인정보를 바이러스, 해킹과 같은 네트워크 침해를 통해 탈취하고, 이를 빌미로 돈을 요구하는 사이버 공격으로 성격이 바뀌고, 급증하여 피해가 커지고 있다.

이런 네트워크 침해를 대비하는 가장 효율적인 기술로써 VPN(Virtual Private Network)이 있다. VPN은 모든 사람들이 사용가능한 공중망(Public Network)을 내부의 사람들만 사용 가능한 사설망(Private Network)처럼 사용할 수 있도록 하는 기술이다. 본 논문에서는 리눅스(Linux) 서버 환경에 적용 가능한 VPN 기술과 관련 프로토콜을 분석하고 최적의 VPN을 제시하였다.

ABSTRACT

While hackers in early days intended to disable and devastate the system, these days people hack and attack the network in order to steal customer's private information from the big corporate, which changes the nature of the crime to cyber attack for money, eventually causing a lot of damages.

One of the most efficient ways to protect this kind of network attack is VPN, referring to Virtual Private Network. VPN is a private networking technology that makes the public network available for only those who are concerned. This paper will suggest the VPN technology that can be applied to Linux server and related protocols and figure the applicable VPN out.

키워드

공중망(Public Network), 사설망(Private Network), 리눅스(Linux), VPN, 프로토콜(Protocol)

Ⅰ. 서 론

2008년 옥션 해킹, 2011년 네이트 해킹, 2014년 3대 카드사 해킹에 이어 2016년 5월 인터넷 쇼핑몰 인터파크의 해킹으로 회원정보 2665만 8753건이 유출되는 사고가 발생하였다. 인터파크를 해킹한 해커는 30억 원 상당의 비트코인을 요구하였다. 또한 우리나라 뿐만 아니라 스위스에서도 은행을 해킹한 해커가 만 유로를 내놓지 않으면 고객 개인정보를 인터넷에 공개하겠다고 은행을 협박했다.

초기의 해커들은 시스템 장애, 파괴가 목적이었으나 최근에는 기업들이 가지고 있는 고객의 개인정보를 바이러스, 해킹과 같은 네트워크 침해

를 통해 탈취하고, 이를 빌미로 돈을 요구하는 사이버 공격으로 성격이 바뀌고, 급증하여 피해가 커지고 있다.

표 1. 기업의 네트워크 침해로 인한 개인정보 유출 피해자 규모

연도	유출사	피해자 규모
2008년	옥션	1000만명
2011년	넥슨	1320만명
2011년	네이트	3500만명
2014년	KT	1170만명
2014년	롯데카드	2600만명
2014년	NH농협카드	2500만명
2014년	KB국민카드	5300만명
2016년	인터파크	1030만명

본 논문의 구성은 다음과 같다. 2장에서 VPN 서버의 필요성과 VPN 관련 프로토콜을 분석하고 3장에서는 리눅스(Linux) 서버 환경에서 최적의 VPN을 제시한다. 마지막으로 4장에서 결론과 향후 연구방향에 대해서 기술한다.

II. VPN 기술 분석

2.1 VPN

기업의 네트워크 침해 공격에 가장 안전한 방법은 기업 내부의 사람들만 사용 가능한 사설망을 구축하여 외부의 접근을 제한하는 것이다. 하지만 사설망은 본사와 지사간의 연결이나 출장, 재택근무 같이 기업 외부에서 기업의 사설망에 연결이 필요할 때 문제가 발생하게 된다. 왜냐하면 기업 외부와 연결을 하기위해 사설망을 확장하려면 전용선 구축이 선행되어야 하고, 전용선을 구축하는데 고가의 임대료가 발생되어 경제적으로 비효율적이기 때문이다. 또한 전용선 대신 공중망을 통해 기업 외부와 연결을 하게 되면 네트워크 침해의 가능성이 생겨 사설망을 사용하는 취지에 부합하지 않게 된다. 이런 상황에서 경제적인 이유와 네트워크 침해 가능성 두 가지를 모두 해결할 수 있는 방법이 VPN(Virtual Private Network)이다.

VPN이란 모든 사람들이 사용가능한 공중망(Public Network)을 내부의 사람들만 사용 가능한 사설망(Private Network)처럼 사용할 수 있도록 하는 기술로써 공중망을 통해 기업 외부와 연결되지만 사용자 인증절차를 수행한 뒤 암호기법을 사용하여 마치 전용선으로 연결된 것과 같은 서비스를 제공하여 보안 문제를 해결 할 수 있다. 또한 고가의 전용선 임대료 대신 상대적으로 저렴한 공중망을 사용하기 때문에 매우 경제적이다 [1].

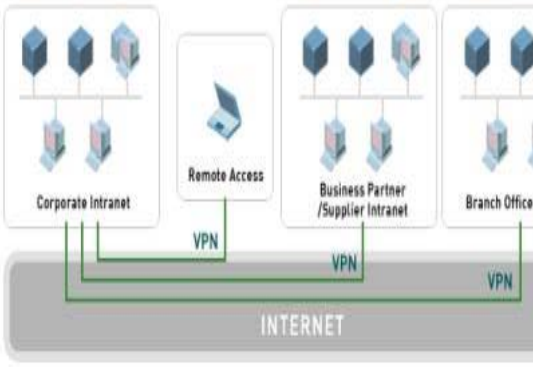

그림 1. VPN 네트워크 구성

2.2 VPN 관련 프로토콜 분석

VPN의 핵심인 VPN 터널링 프로토콜은 데이터 패킷의 암호화, 터널의 생성 및 관리, 암호화 키의 관리를 수행한다. 터널링 프로토콜은 라우팅 정보가 추가된 헤더와 개인데이터를 캡슐화하고 캡슐화 된 프레임은 헤더에 추가되어 있는 라우팅 정보를 기반으로 공중망을 경유하여 전송되고 목적지에 도달하면 디캡슐화 되어 최종 목적지로 향하게 된다.

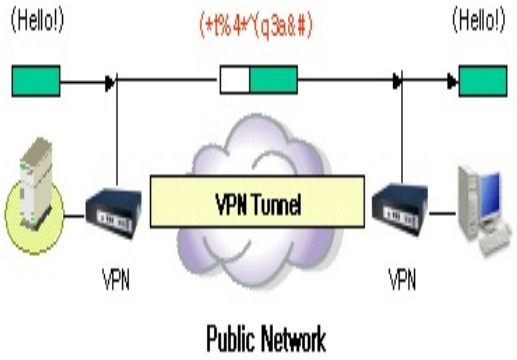

그림 2. 터널링 기법

대표적인 VPN 프로토콜로 IPSec(IP Security), SSL(Secure Sockets Layer), L2TP(Layer 2 Tunneling Protocol), PPTP(Point-to-Point Tunneling Protocol) 등이 있다.

IPSec은 OSI 계층 Layer 3 프로토콜이며 인증 헤더 AH(Authentication Header)와 인증과 데이터 암호화를 함께 지원하는 ESP(Encapsulating Security Payload), 키교환을 위한 IKE(Internet key exchange)등을 이용해 보안 서비스를 제공한다. IPSec을 사용하기 위해서는 원격 사용자의 장치에 VPN 소프트웨어를 설치하거나 네트워크 게이트웨이로 동작 하는 하드웨어 클라이어언트 장치를 설치해야 한다. IPSec 기반의 VPN은 HTTP, FTP, ICMP, SMTP, VoIP와 같은 모든 IP 서비스를 지원하

고 있다[2][3].

SSL은 넷스케이프에서 개발된 프로토콜로서 OSI 계층 Layer 5 프로토콜이기 때문에 기존의 커널을 수정하지 않고 웹 브라우저만 있으면 사용할 수 있다. SSL은 다양한 장점을 지닌 암호화 기법들을 사용해 세계 각국에서 사용되는 대부분의 암호화 기법들을 지원한다.

PPTP는 PPP(Point-to-Point) 접속을 확장하여 원격 사용자와 사설망 사이의 보안 접속을 제공하는 OSI 계층 Layer 2 프로토콜로써 인터넷 프로토콜인 TCP/IP를 그대로 이용하면서 외부인이 접근할 수 없는 VPN을 구축할 수 있도록 해주는 프로토콜이다. PPTP를 사용하여 VPN사용자는 PPP방식으로 서버에 접속한 후 인증을 받으면 VPN 터널이 생성되고 이를 통해 VPN 연결이 가능해진다. 주로 외부에서 사내의 서버에 접속하기 위해 널리 이용되며 다양한 OS에서 기본적으로 제공하고 있다.

L2TP는 L2F(Layer 2 Forwarding)와 PPTP를 결합한 것으로, OSI 계층 Layer 2 프로토콜이다. PPTP와 달리 L2TP에서는 MPPE를 사용하여 PPP데이터그램을 암호화하지는 않는다. 또한 UDP 뿐만 아니라 IP전송계층이 없는 WAN 구간에서도 사용이 가능하며 X25, 프레임 릴레이, ATM(Asynchronous Transfer Moder)등 다양한 네트워크를 지원한다.

III. 리눅스 VPN 프로그램 분석

초기의 VPN은 PPTP, L2TP기반의 VPN이 사용었으나, 보안이 강화된 IPSec 기반의 VPN인 FreeSWAN, Openswan등이 대표적인 리눅스의 VPN으로 자리를 잡았다. 하지만 FreeSWAN의 개발은 중단되었고, FreeSWAN의 개발을 이어받은 Openswan또한 개발이 활발하게 이루어지지 못하고 있다. 뿐만 아니라 IPSec 기반의 VPN은 설치 및 설정이 어렵고, 호환성 부분에서도 문제가 발생하여 최근에는 SSL 기반의 OpenVPN이 대세를 이루고 있다[4][5].

OpenVPN은 다양한 특징을 가지고 있는데 첫째 하나의 UDP 또는 TCP 포트를 통해 IP Subnet이나 가상의 이더넷 트래픽을 터널링할 수 있다. 예를 들면 5000/udp 한 포트를 통해 FTP도 접속하고 웹 접속도 하고, Ping도 이용할 수 있다

둘째 안전한 VPN 통신을 위해 openssl에서 지원하는 강력한 암호화, 인증기능을 그대로 이용할 수 있다. 그리고 미리 지정된 키를 공유해 상호인증을 하거나 https처럼 인증서를 통해 인증할 수도 있을 뿐만 아니라 추가적으로 아이디/패스워드를 이용한 인증기능도 지원한다.

셋째 설치와 설정이 복잡하고 어려운 PPTP나 L2TP/IPSec에 비해 OpenVPN은 시스템 내에 별도의 데몬 형태로 작동하기 때문에 복잡한 커널 패치나 커널 모듈이 필요하지 않고, 설치방법이 매우 쉽다.

넷째 모든 패킷이 VPN을 통과함에도 불구하고 시스템에 부하를 유발하지 않으면서 속도도 빠르다[6].

	Basic VPN PPTP	STANDARD VPN L2TP/IPsec	SECURE VPN OpenVPN
Encryption/Security	128 BIT Basic	256 BIT Standard	2048 BIT Very Strong
Supported OS	Windows Mac OS X Linux iOS Android Windows Mobile DD-WRT	Windows Mac OS X Linux iOS Android Windows Mobile DD-WRT	Windows Mac OS X Linux iOS Android Windows Mobile DD-WRT
Compatibility	desktops, laptops, tablets, smartphones	desktops, laptops, tablets, smartphones	desktops, laptops, tablets, smartphones
Speed	very fast due to the basic encryption	requires more CPU to encrypt data	best performance, very fast even on connection with high delay
Configuration	very simple, the protocol built into most devices, does not require additional software	simple, requires additional settings, the protocol built into most devices, does not require additional software	additional software required, optionally need to install certificates
Ports	TCP 1723	UDP 500 UDP 1701 UDP 4500	ANY (highly customizable, can use any ports available, can listen both TCP and UDP protocol)
Ability to Fuck GFW	least reliable, very easy to be blocked/filtered	not reliable, still very easy to be blocked/filtered	very flexible and customizable, very difficult to be blocked/filtered
Summary	PPTP is very fast and very easy to set up. It is a good choice if your device does not support OpenVPN or SSTP VPN, and security is not one of your concerns.	L2TP/IPsec is a good choice if your device does not support OpenVPN or SSTP VPN and you care about the slightly higher security.	OpenVPN is the recommended protocol for all platforms, the highest performance, security and reliability.

그림 3. PPTP, L2TP/IPSec, OpenVPN 비교

IV. 결 론

VPN의 구성으로 본사와 지사간의 연결이나 출장, 재택근무 같이 기업 외부에서 기업체 사설망에 연결이 필요할 때 저렴한 비용과 더불어 사용자 인증절차와 암호기법을 통해 전용선을 구축한 것과 같은 효과를 얻을 수 있다. 또한 SSL기반의 OpenVPN을 이용하여 리눅스 서버 환경에서 PPTP, L2TP, IPSec에 비해 높은 호환성과 쉬운 설치 및 설정으로 간단하게 VPN을 구성할 수 있을 뿐만 아니라 높은 보안성과 속도, 낮은 시스템 부하를 통해 안정적으로 VPN을 운영하여 네트워크 침해를 효과적으로 대비할 수 있다.

향후 연구과제로는 분석한 OpenVPN을 이용해서 VPN을 설계하고 구현하여 사용자 인증과 암호화를 통한 네트워크 침해 대비에 관련하여 시스템 보안 평가 형태의 연구가 필요하다.

감사의 글

본 논문은 중소기업청의 2016년도 기업서비스 연구개발사업(과제번호: S2369585)의 연구 결과로 수행되었음

참고문헌

[1] 정성재, 배유미, 이광용, “리눅스 관리 및 시스템보안(리눅스 실무 마스터가 되기 위한)”, 북스홀릭 퍼블리싱, pp. 371, 2016년.
[2] http://www.ipsec.com
[3] http://www.ietf.org/html.charters/ipsec-charter.html
[4] http://www.freeswan.org/
[5] http://www.openswan.org/
[6] http://openvpn.sourceforg.net